CLAIMS

What is claimed is:

1. A method for authenticating network entities in a fibre channel network, the method comprising:

receiving a fibre channel authentication message from a first network entity at a second network entity in a fibre channel network, wherein the authentication message provides information for authenticating or reauthenticating the first network entity in the fibre channel network;

determining that both the first network entity and the second network entity support security;

verifying that the first network entity corresponds to an entry in an authentication table associated with the second network entity;

receiving first network entity verification information that confirms the identify of the first network entity.

2. The method of claim 1, further comprising generating a session key at the second network entity, wherein the session key is generated using public information associated with the first network entity and a random parameter.

3. The method of claim 1, further comprising:

exchanging security association parameters such as the SPI and the algorithm identifier.

4. The method of claim 1, wherein the authentication message is associated with a request for a fabric login.

5. The method of claim 1, wherein determining that both the first and second network entities support security comprises identifying a security enable parameter in the initialization message.

6. The method of claim 1 further comprising determining which authentication and key exchange protocol are supported by the two entities.

7. The method of claim 2, wherein the public information associated with the first network entity is provided to the second network entity by the first network entity.

8. The method of claim 2, wherein the session key generated at the second network entity is also generated at the first network entity using public

information associated with the second network entity and a random parameter provided by the second network entity.

9. The method of claim 8, wherein the public information associated with the second network entity is provided to the first network entity by the second network entity.

10. The method of claim 8, wherein first network entity verification information is generated at the first network entity using public information associated with the first and second network entities and the session key.

11. The method of claim 10, further comprising verifying that the first network entity verification information received corresponds to verification information generated at the second network entity using public information associated with the first and second network entities and the session key.

12. The method of claim 11, further comprising transmitting second network entity verification information to the first network entity, wherein the second network entity verification information is generated at the second network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

13. The method of claim 12, wherein the second network entity verification information transmitted corresponds to second network entity verification information generated at the first network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

14. The method of claim 8, wherein the second network entity is a storage device in a storage area network.

15. The method of claim 8, wherein the first and second network entities are domain controllers in a storage area network.

16. The method of claim 8, wherein the first and second network entities are switches.

17. The method of claim 8, wherein the first network entity is a host.

18. The method of claim 17, wherein the second network entity is a storage device.

19. The method of claim 8, wherein the authentication message is a fibre channel authentication message.

20. The method of claim 19, wherein the authentication message is a login message.

21. The method of claim 20, wherein the authentication message is a PLOGI or FLOGI message.

22. The method of claim 8, further comprising:

storing security association information associated with the first network entity.

23. The method of claim 8, further comprising:

transporting security association information in the messages exchanged between the two network entities

24. The method of claim 22, wherein security association information comprises an identifier associated with the first network entity and the session key.

25. The method of claim 24, wherein security association information further comprises an encryption algorithm identifier and an authentication algorithm identifier.

26. A method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a frame at a first network entity from the second network entity in a fibre channel network;

identifying a security control indicator in the frame from the second network entity;

determining that a security association identifier associated with the frame corresponds to an entry in a security database;

decrypting the first portion of the frame by using algorithm information contained in the entry in the security database.

27. The method of claim 26, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

28. The method of claim 27, wherein the first portion is decrypted using a key contained in the entry in the security database.

29. The method of claim 27, wherein the first portion is encrypted using DES, 3DES or AES.

30. The method of claim 27, further comprising:

recognizing that a second portion of the frame supports authentication;

using algorithm information contained in the entry in the security database to authenticate the second portion of the frame.

31. The method of claim 30, wherein the second portion is authenticated using MD5 or SHA1.

32. The method of claim 30, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

33. The method of claim 32, wherein the login sequence is a PLOGI or FLOGI sequence.

34. The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence.

35. The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a SW_ILS sequence.

36. A method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

transmitting the fibre channel frame to the second network entity.

37. The method of claim 36, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

38. The method of claim 36, wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol.

39. The method of claim 38, further comprising adding security information to the header of the fibre channel frame.

40. The method of claim 37, wherein a first portion of the fibre channel frame is encrypted using DES, 3DES, or AES.

41. The method of claim 37, wherein parameters in the header are normalized prior to encrypting the first portion of the fibre channel frame.

42. The method of claim 41, wherein the payload is padded prior to encrypting the first portion of the fibre channel frame.

43. The method of claim 37, further comprising:

computing authentication data using key and algorithm information as well as a second portion of the fibre channel frame.

44. The method of claim 43, wherein authentication data is computed using MD5 or SHA1.

45. The method of claim 43, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

46. The method of claim 45, wherein the login sequence is a PLOGI or FLOGI sequence.

47. The method of claim 45, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW_ILS message.

48. An apparatus for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

means for encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

means for transmitting the fibre channel frame to the second network entity.

49. The apparatus of claim 48, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

50. An apparatus for receiving encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying that the frame has been secured

means to lookup the security parameters in a security database that allow the de-encapsulation of the frame

means to decrypt the eventually encrypted frame

means to verify that the message has been sent by the sender, and that has not been tampered during its transmission

5